CLAIMS

1. Method for documenting a transfer of authority of control for a container from a first entity of a transportation chain to a second entity of the transportation chain,
wherein the first entity transfers an electronic container control certificate to an electronic seal of the respective container, which electronic container control certificate comprises a cryptographic key associated to the second entity, and which container control certificate is digitally signed by the first entity.

2. Method according to claim 1, comprising
storing the container control certificate in a log of the electronic seal.

3. Method according to claim 1 or claim 2, comprising
verifying the signed container control certificate by a corresponding function implemented in the electronic seal.

4. Method according to claim 3, comprising
verifying the digital signature of the container control certificate by applying decrypt information stored in the log of the electronic seal and delivered to the log by a previous entity of the transportation chain.

5. Method according to claim 4,
wherein the verification is considered to be failed if the signed container control certificate cannot be decrypted with the decrypt information stored in the log.

6. Method according to any one of the claims 3 to 5,
wherein a status of a container lock is subject to the result of the signature verification process.

7. Method according to any one of the claims 3 to 6,
wherein the electronic seal issues a warning if the verification of the signature fails.

8. Method according to any one of the claims 3 to 7,
wherein the container control certificate is stored in the log if the verification succeeds.

9. Method according to any one of the previous claims,
wherein the cyptographic key associated to the second entity is used by the electronic seal for decrypting data expected to be received from the second entity.

10. Method according to any one of the previous claims,
wherein the electronic seal is designed for controlling a lock of the container.

11. Method according to any one of the previous claims,
wherein an asymmetric cryptographic key system is used for digitally signing the container control certificate.

12. Method according to claim 11,
wherein a public - private key system is used for digitally signing the container control certificate.

13. Method according to claim 12,
wherein the container control certificate is signed using a private key associated to the first entity.

14. Method according to claim 4 in combination with claim 13,
wherein the decrypt information stored in the log comprises a public key of the first entity.

15. Method according to any one of the previous claims,
wherein the first entity receives the cryptographic key associated to the second entity from a certificate authority.

16. Method according to any one of the previous claims,
wherein the container control certificate comprises identification data for the container.

17. Method according to any one of the previous claims,
wherein a location recording device associated to one of the entities transfers location data to the electronic seal.

18. Method according to claim 17,
wherein the location data is digitally signed by the associated entity.

19. Method according to claim 17 or claim 18,
wherein the signed location data is stored in a log of the electronic seal.

20. Method according to one of the preceding claims 17 to 19, comprising
verifying the signed location data by a corresponding function implemented in the electronic seal.

21. Method according to claim 20 comprising
verifying the digital signature of the location data by applying decrypt information stored in the log of the electronic seal and delivered to the log by a previous entity of the transportation chain.

22. Method according to claim 20 or claim 21,
wherein the verification is considered to be failed, if the signed location data cannot be decrypted with decrypt information stored in the log.

23. Method according to any one of the claims 20 to 22,
wherein recording the location data in the log of the electronic seal is subject to a result of the signature verification process.

24. Method according to any one of the previous claims,
wherein the electronic seal transmits container identification information to a location recording device associated to one of the entities.

25. Method according to claim 24,

wherein the transmitted container identification information is digitally signed by ??

26. Computer program element comprising computer program code means for performing a method according to any one of the preceding claims when into a processing unit.

27. Computing unit for communicating with an electronic seal of a container, the computing unit comprising

- an interface for transferring data to the electronic seal, and
- a control unit designed for
    - assembling an electronic container control certificate, the container control certificate comprising a cryptographic key associated to an entity different from the entity the computing unit is associated to,
    - digitally signing the container control certificate on behalf of the associated entity, and
    - submitting the digitally signed container control certificate to the interface.

28. Computing unit according to claim 27, comprising

- an interface for communicating to a certificate authority;
- the control unit being designed for requesting the cryptographic key associated to the different entity from the certificate authority.

29. Computing unit according to claim 18, comprising

a log for storing a cryptographic key associated to the certificate authority for decrypting information received from the certificate authority via the certificate authority interface.

30. Electronic seal for a container, comprising

- an interface accessible for entities participating in the transportation chain,
- a log for recording data, and
- a control unit for verifying data received via said interface, the control unit being designed for decrypting a digitally signed electronic container control certificate received via said interface, the decryption process using decrypt information stored in the log which decrypt information being associated to the transmitting entity.

31. Electronic seal according to claim 30,
wherein the control unit is designed for storing the signed container control certificate in the log.

32. Electronic seal according to claim 30 or claim 31,
wherein the control unit is designed for considering the verification being failed if the signed container control certificate cannot be decrypted with the decrypt information stored in the log.

33. Electronic seal according to any one of the preceding claims 30 to 32,

- wherein the control unit is designed for controlling a lock of the associated container, and
- wherein a status of the container lock is subject to the result of the signature verification process.

34. Electronic seal according to any one of the preceding claims 30 to 33,
wherein the control unit is designed for issuing a warning if the verification of the signature is considered to be failed.

35. Electronic seal according to any one of the preceding claims 30 to 34,
wherein the control unit is designed for storing the container control certificate in the log if the verification succeeds.

36. Electronic seal according to any one of the preceding claims 30 to 35,
wherein the decrypt information comprises a public key of the first entity in case a private - public key signing mechanism is used for signing the container control certificate at the transmitting entity.

37. Electronic seal according to any one of the preceding claims 30 to 36, comprising an interface for communicating with a location recording device associated to one of the entities, the control unit being designed for receiving location data from the location detection device via said interface.

38. Electronic seal according to claim 37,
wherein the control unit is designed for storing the received location data in the log.

39. Electronic seal according to claim 37 or claim 38,
wherein the control unit is designed for verifying a digital signature of the received location data by a corresponding function.

40. Electronic seal according to claim 39,
wherein the control unit is designed for verifying the digital signature of the location data by applying decrypt information stored in the log and delivered to the log by a previous entity of the transportation chain.

41. Electronic seal according to claim 39 or claim 40,
wherein the control unit is designed for considering the verification to be failed if the signed location data cannot be decrypted with the decrypt information stored in the log.

42. Electronic seal according to any one of the preceding claims 39 to 41,
wherein the control unit is designed for a storing the location data in the log subject to the result of the signature verification process.

43. Electronic seal according to any one of the preceding claims 30 to 42
wherein the control unit is designed for transmitting container identification information to a remote location recording device associated to one of the entities.

44. Electronic seal according to claim 43,
wherein the control unit is designed for digitally signing the container identification information before the transmittal.

45. Method for documenting a transfer of authority of control for a container from a first entity of a transportation chain to a second entity of the transportation chain in an electronic

seal for the container, the method comprising steps as performed by the control unit according to any one of the previous claims 30 to 44.

46. Computer program element comprising computer program code means for performing a method according to claim 45 if loaded into the processing unit of an electronic seal.

47. System for documenting a transfer of authority of control for a container from a first entity of a transportation chain to a second entity of the transportation chain, the system comprising:

- a computing unit according to any one of the claims 27 to 29, which computing unit is associated to the first entity, and
- an electronic seal according to any one of the claims 30 to 44, which electronic seal is associated to the container.

48. System for documenting transfer of authority of control for a cargo container from a first entity of a transportation chain to a last entity of the transportation chain, the transportation chain comprising one or more further participating entities, the system comprising:

- a computing unit associated to the entities transferring authority of control, each of the computing units being designee according to any one of the claims 27 to 29, and
- an electronic seal according to any one of the claims 30 to 44, which electronic seal is associated to the container.

49. System according to claim 47 or claim 48, comprising
a certificate authority for supporting the computing unit with cryptographic data as needed.

50. Method for documenting a transfer of authority of control for a cargo container from a first entity of a transportation chain via one or more further entities to a last entity of the transportation chain,
wherein each entity transferring authority of control transfers an individual electronic container control certificate to an electronic seal of the respective container during the course of transferring authority of control between the entities, which individual electronic container

control certificate comprises a cryptographic key associated to the respective next entity in the transportation chain, and which container control certificate is digitally signed by the transferring entity.

51. Method according to claim 50,
wherein each individual container control certificate is stored in a log of the electronic seal.

52. Method according to claim 50 or claim 51,

- wherein the entity providing the container issues identification data for the container and transfers such identification data to the electronic seal, and
- wherein the electronic seal stores the identification data in its log.

53. Method according to any one of the preceding claims 50 to 52,

- wherein the entity providing the container issues an electronic container provider certificate, digitally signs this container provider certificate with a key associated to a certificate authority and transfers the signed container provider certificate to the electronic seal, and
- wherein the electronic seal stores the container provider certificate or in its log.

54. Method according to any one of the preceding claims 50 to 53,

- wherein the entity supplying the cargo issues an electronic cargo manifest which cargo manifest comprises data on the cargo to be delivered, digitally signs the cargo manifest and transfers the signed cargo manifest to the electronic seal, and
- wherein the electronic seal stores the cargo manifest or the signed cargo manifest in its log.

55. Computer program element comprising computer program code means, which code means when loaded in a processor unit perform a method according to any one of the preceding claims 50 to 54.

56. Location recording device for recording a track of a container, comprising

- a location detector for detecting the actual location,

- a log for recording location data,
- an interface for communicating with an electronic seal of a remote container to be tracked, and
- a control unit designed for
    - recording location information to the log, and for
    - exchanging data with the electronic seal via the interface.

57. Location recording device according to claim 56
wherein the exchange of data comprises transmitting the detected location data to the electronic seal.

58. Location recording device according to claim 56 or claim 57
wherein the exchange of data comprises receipt of container identification information from the electronic seal.

59. Location recording device according to ant one of the preceding claims 56 to 58, wherein the location detector comprises a global positioning module for determining the actual location.

60. Location recording device according to any one of the preceding claims 56 to 59, wherein the control unit is designed for recording location information together with a time stamp.

61. Location recording device according to any one of the preceding claims 56 to 60, wherein the control unit is designed for providing the location information with a digital signature.

62. Electronic seal for a container, comprising
- an interface for communicating with a remote location recording device, and
- a control unit for verifying data received via said interface, the control unit being designed for

    decrypting digitally signed location data received via said interface.

63. Electronic seal according to claim 62, comprising

- a log for recording data,
- wherein the control unit is designed for recording received location data if the signed location data can be decrypted by means of decrypt information stored in the log.

64. Method for recording a track of a container on its way from a first location to a second location, comprising

at a location recording device:

- detecting the actual location,
- recording the location data in a log, and
- transferring this location data to an electronic seal of the container;

at the electronic seal of the container:

- receiving the location data, and
- recording the location data in a log of the electronic seal.

65. Method according to claim 64,

- wherein the location data is digitally signed before transmitted to the electronic seal, and
- wherein the signature is verified at the electronic seal.

66. Method according to claim 64 or claim 65,

wherein the location data is recorded together with a time stamp.

67. Method according to any one of the preceding claims 64 to 67,

wherein a risk manager checks the records of the location recording device.

68. Method according to claim 67,

wherein the risk manager compares the records of the location recording device with the records of the seal's log.

69. Method according to claim 68,
wherein the risk manager issues a note if the records of the location detection unit and the records of the container differ.

70. Method for recording a track of a container on its way from a first location to a second location, comprising
at a location recording device:

- detecting the actual location,
- receiving container identification information from an electronic seal of a container, and
- recording the location data together with the container identification information in a log.

71. Computer program product comprising computer program code means for performing a method according to any one of the previous claims 64 to 70 when loaded in a processor unit.